



FOURTH AMENDMENT · RESOURCES

Hash Hits, Human Eyes, and the Limits of Private Search in United States v. Lowers

By Daigle Law Group

August 11, 2026

DAIGLE LAW GROUP

This publication is produced to provide general information on the topic presented. It is distributed with the understanding that the publisher is not engaged in rendering legal or other professional services. Always consult qualified counsel for advice specific to your situation.

dlglearningcenter.com

Hash Hits, Human Eyes, and the Limits of Private Search in *United States v. Lowers*

By Daigle Law Group · August 11, 2026

In a recent case from the Fourth Circuit, the Court examined *United States v. Lowers*, a case that highlights privacy in the digital age and reiterates that individuals have a reasonable expectation of privacy in files they store in their private cloud accounts.

Summary of the Facts

In September 2019, 156 files were uploaded to the user “harvardeperstein@gmail.com’s” Google Drive account. Once uploaded, Google began its process of hash matching. Hashing creates a digital fingerprint for a file. Hash matching compares that fingerprint against a database of known files to determine whether there is a match. If there is a match, it strongly suggests the file is the same one already identified, even if it has been copied or renamed. This helps investigators quickly find known material without having to view every file, saving time and reducing unnecessary exposure. Google’s hashing algorithm determined that each file matched a known hash value in its apparent child sexual abuse material repository. A trained Google reviewer opened 31 files and concluded that they all contained CSAM. A CyberTip report was compiled, identified which files were reviewed and which files remained unopened and unreviewed, and was sent to the National Center for Missing and Exploited Children. An NCMEC employee received all 156 files with the report and reviewed the same 31 files as the Google reviewer. No additional files were opened. Because the employee believed that the IP address corresponded to Bedford County, Virginia, the report was forwarded to the Bedford County Sheriff’s Office in October. In April 2020, an investigator finally reviewed the report and discovered that the IP address was linked to a Chesapeake address. The investigator closed the file and sent the report to the Chesapeake Police Department.

Upon receiving the report, Detective Rider downloaded it. Without obtaining a warrant, she opened and viewed at least three files that had not yet been opened or viewed. Each file contained CSAM, so Rider applied for a search warrant for the Google account based on the three files she had opened without a warrant. The warrant revealed that the account was created, used to upload the files, and never used again. In September, Rider applied for a search warrant for the home, describing the files she had viewed without a warrant. In October, the warrant was executed and revealed a married couple and their children living at the address. None of the ten seized devices contained CSAM. During the husband’s voluntary interview, he informed officers that their 21-year-old son, Nico Lowers, had

recently moved out. He provided them with his son's phone number and new address in Raleigh, North Carolina. Chesapeake Police closed their file and sent all their information to the Raleigh Police Department. In November, Homeland Security Agent Covington contacted Lowers, and Lowers consented to a voluntary interview at his apartment. When Agent Covington and Raleigh Police Detective Faust asked about the Google Drive account, Lowers claimed ignorance but consented to a search of his cell phone and laptop. The forensic analysis of Lowers' devices recovered four videos containing CSAM from the deleted files on Lowers' phone. After being contacted, Lowers consented to a second interview. In December, Lowers was interviewed at RPD, where he initially continued to claim ignorance. When confronted with the discovered CSAM, he confessed to downloading CSAM onto a flash drive at his parents' home and bringing it with him. Lowers then told officers where they could find the flash drive in his apartment. Simultaneously, officers were executing a search warrant for Lowers' apartment. Two officers left the interview to retrieve the flash drive and also recovered a hard drive. Combined, the flash drive and hard drive contained 1,028 images and 28 videos, each depicting CSAM.

Lowers was charged with transporting and possessing CSAM. However, the charges were unrelated to the files uploaded to his Google Drive account and instead related to the CSAM discovered at his apartment. He moved to suppress all evidence against him, arguing multiple Fourth Amendment violations. The district court denied the motion, finding that no search had occurred. The court also held that, even if there had been an unconstitutional search, the attenuation doctrine applied. Lowers entered a conditional guilty plea and appealed to the Fourth Circuit.

United States Court of Appeals for the Fourth Circuit

The court first examined whether Lowers had a reasonable expectation of privacy in his Google Drive. Under *Katz*, the defendant must show a subjective expectation of privacy and that the expectation is one society recognizes as reasonable. On appeal, the court examined whether it was objectively reasonable for Lowers to have such an expectation of privacy. Here, Google's privacy policy states that "Google may 'analyze their content to help Google detect abuse such as spam, malware, and illegal content.'" The court found that this diminished any Google Drive user's reasonable expectation of privacy. However, "a diminished privacy interest does not mean that the Fourth Amendment falls out of the picture entirely." Based on Google's privacy policy, the Fourth Circuit concluded that Google Drive users agree to Google, not the government, analyzing their content. Therefore, the court concluded that the government does not have the same authority to do so.

The court then examined whether the private search doctrine allowed Rider to open and view three unopened files without a warrant. The private search doctrine allows a private party to conduct its own

search. If the private party discovers evidence of a crime, it can turn that evidence over to the police, who do not need to “avert their eyes.” However, police cannot exceed the scope of the original search. Here, no one at Google opened the three specific files that were opened by Rider. Although Google’s hash-matching process suggested that the three files contained CSAM, the algorithm revealed nothing about the images themselves and only assigned a serial number. Rider, however, learned the actual visual contents of the files when she opened them. Thus, the court concluded that Rider’s visual examination of the files provided her with new information and was therefore unconstitutional. Because Lowers also sought suppression of the flash drive, hard drive, and confession as stemming from Rider’s unconstitutional search, the court examined whether the attenuation doctrine applied.

Under the attenuation doctrine, evidence is admissible when the connection between unconstitutional police conduct and the evidence is remote or has been interrupted by an intervening circumstance. It depends on how much time has passed between the illegal search and the acquisition of the evidence, whether there were any intervening circumstances, and the purpose and flagrancy of the officer’s misconduct. Here, seven months elapsed between Rider’s illegal search and the later-discovered evidence. Moreover, Lowers voluntarily agreed to two interviews, consented to the search of his laptop and phone, confessed, and told officers where to find the flash drive. Thus, the court found that the first two prongs favored attenuation. For Rider’s conduct to be “flagrant,” she would have had to commit an “abusive violation of the Fourth Amendment.” Here, she viewed unopened files without a warrant, making it an unconstitutional search. However, there was no evidence that Rider did so to avoid the warrant requirement. Thus, the third prong also favored attenuation. Therefore, the court found that the attenuation doctrine applied. Ultimately, even though the court found Rider’s search unconstitutional, the later evidence was not suppressed, and the court upheld Lowers’ conviction.

Key Takeaways

Lowers emphasizes that, although private cloud storage may carry a diminished expectation of privacy because of a provider’s privacy policy, a warrant is still required for a police officer to review those files. Any files reviewed by a private party may be reviewed without a warrant by law enforcement under the private search doctrine. However, it is crucial that law enforcement not exceed the scope of what the private party has already done, or else the private search doctrine will not apply. In this case, the attenuation doctrine applied only because of the passage of time, consent, and other intervening events, not because the search of unopened files was lawful.

***United States v. Lowers*, No. 24-4546 (4th Cir. 2026)**